UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,004	05/22/2002	Masahiro Mimura	566.40671X00	2837

24956 7590 04/14/2006

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
TUCKER, WESLEY J	

ART UNIT	PAPER NUMBER
2624	

DATE MAILED: 04/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/937,004	MIMURA ET AL.	
	Examiner	Art Unit	
	Wes Tucker	2624	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 5-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 5-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 July 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 31st 2006 has been entered.

Response to Amendment

2. Applicants amendment filed March 31st 2006 has been entered and made of record.

3. Applicant has amended claims 1, 7, 10. New claims 11-21 have been added. Claims 1 and 5-21 are currently pending.

4. Applicants remarks in view of the newly presented claims and amended claims have been considered and are found at least partially persuasive. However the amendments have changed the scope of the claims and have necessitated a new rejection using the addition of the reference of U.S. Patent 6,241,288 to Bergenek et al.

5. The amendment will now be summarized as interpreted by Examiner.

Applicant has amended the independent claims to include the new limitations of:

wherein the transmitting means of the reader/writer comprises, for each partial image;

means for extracting from the input fingerprint a partial image requested by the requesting means of the mobile storage device, means for transmitting the extracted partial image to the mobile storage device, and means for repeatedly extracting and transmitting each of the partial images one by one until a satisfactory level of matching is achieved, and

wherein the judging means of the mobile storage device comprises:

means for repeating the matching result for each partial image.

As applicant states the difference between the newly claimed limitation and the primary reference to Wiebe is that Wiebe transfers the **entire pre-processed image** to the card for comparison with a template composed of several partial images while the present invention transfers **only partial images taken from a whole image** for performing the matching with the template.

Neither Wiebe Hara nor Iwata disclose transferring only partial images to be matched with a defined template.

Accordingly the new reference to U.S. Patent 6,241,288 to Bergenek et al. is cited to teach the claimed feature of determining correspondence of fingerprints using only partial images to match with a template. Bergenek discloses matching fingerprints in the same smart card environment (column 1, lines 15-25). Bergenek further discloses using partial images to determine if an inputted image matches a template

image to a certain degree, wherein the template is made up of partial images as well (column 15, lines 42). Bergenek also teaches that the partial images are compared one by one in the discussion of outlying regions (column 15, lines 14-30).

Bergenek further teaches an advantage of using partial images instead of the entire fingerprint images if the security of not transmitting the entire fingerprint image. The added bonus of lessened computation time and expense in performing fewer pixel-to-pixel comparisons is also and obvious advantage. Therefore it would have been obvious to one of ordinary skill in the art at the time of invention to use the partial image matching taught by Bergenek in order to lessen computation time as well as provide added security.

It should be noted that Applicant has also amended the independent claims to change matching small images in the image and template to partial images in the image and template. The reference of Wiebe is still interpreted to read on this limitation because the template is composed of partial images and therefore only partial images from the input image will actually be matched.

Claim Rejections - 35 USC § 112

6. The previously presented 112 rejection of claim 7, is withdrawn in view of applicant's amendments.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1 and 5-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of U.S. Patent 6,719,200 to Wiebe, Japanese Patent Application Publication No. 06-301768 (Application No. 05-086477): Fingerprint Collation Device, Publication Date: October 1994) to Iwata, hereinafter referred to as Iwata, and U.S. Patent 5,040,224 to Hara and further in view of U.S. Patent 6,241,288 to Bergenek et al.

With regard to claim 1, Wiebe discloses ***an authentication system*** (abstract) ***comprising***:

A mobile storage device (column 3, lines 27-40 and Fig.1, element 1, smart card); and

A reader/writer (Fig.1, element 2) ***for performing at least one of reading information and writing information into said mobile storage device*** (column 10, lines 10-15),

Wherein said reader/writer comprises:

A biological information input device which inputs fingerprint information (Fig.1, element 8).

Wiebe further discloses preprocessing means for calculating coordinates or features of the fingerprint and rotating/translating the fingerprint to better register the stored fingerprint with the input fingerprint (column 5, lines 35-42 and column 6, lines 5-29). Wiebe discloses rotating and translating the image by the use of partial images and features, which must inherently have known coordinates in order to register the images.

Wiebe further discloses ***wherein said mobile storage device comprises:***

A template which registers a plurality of coordinates of featuring points of the fingerprint and small images in vicinity of the coordinates (column 5, lines 7-26 and column 9, lines 14-35). Wiebe discloses using partial images of the fingerprint to register the stored fingerprint with the newly input fingerprint. Knowing the location or coordinates of the partial images is inherent to using the location of image features for registration. The reduced data quantity image used for verification is further stored as a template (column 9, lines 14-18).

Wiebe further discloses ***a private key to be used for electronic authentication*** (column 3, lines 42-50 and column 1, lines 45-54). The sensitive information stored on the smart card may include, though is clearly not limited to a "key" which makes it possible to open a door to access authorized data, so-called digital certificates (column 3, lines 42-50) or more conventional information, such as a personal identification code or PIN (column 1, lines 50-54).

Wiebe further discloses ***calculating means for calculating an information for correcting a positional displacement of an input fingerprint that is newly inputted, referring to a position generated in the reader/writer*** (column 6, lines 15-27).

Wiebe further discloses ***means for calculating coordinates of featuring points of the input fingerprint by calculating information for correcting the positional displacement with each of the coordinates of featuring points and request fingerprint images in the vicinity of the coordinates of featuring points of the inputted fingerprint from the reader/writer*** (column 5, lines 12-34 and column 6, lines 18-28). Wiebe uses partial images or featuring points to compare data between fingerprints and using the partial images or featuring points it can be determined how to translate or rotate one or both of the fingerprints fro comparison.

Wiebe further discloses ***Judging means for judging whether the small images in the vicinity of the coordinates of the fingerprint registered in the template and the small images in the vicinity of the coordinates of featuring points of the inputted fingerprint match*** (column 5, lines 6-25) Wiebe discloses matching the two images using a reduced data content of partial images. Wiebe further discloses ***in accordance with a plurality of results of the matching, judges whether the fingerprint registered in the template and the input fingerprint are identical*** (column 5, lines 20-26). Wiebe describes how verification is achieved using only a selected amount of partial images.

Wiebe further discloses ***Means for making the private key available when the result of judging fingerprints are identical*** (column 1, lines 45-50, column 3, lines 42-

50 and column 5, lines 52-64). Wiebe discloses how once verification is achieved on the fingerprint data certain functions can be performed. Here the private key is interpreted as the act of allowing access to certain sensitive information.

Wiebe further teaches ***a transmitting means for transmitting the position generated in the preprocessing means to said mobile storage device according to a request from said mobile storage device*** (column 6, lines 39-47). The smart card has communication means capable of receiving and transmitting information. Using the determined position to align images is just one of many well-known methods used in the art to align and verify fingerprint images.

Wiebe does not disclose the limitations dealing with the core calculation and alignment of the fingerprint information. Wiebe teaches that any method appropriate for the application for comparing feature information of fingerprint information may be used in the access method taught (column 6, lines 5-9).

Wiebe discloses ***preprocessing means for calculating coordinates or features of the fingerprint and rotating/translating the fingerprint to better register the stored fingerprint with the input fingerprint*** (column 5, lines 35-42 and column 6, lines 5-29). The coordinates are considered inherent to use the known locations of partial images for the registration of the fingerprints. Wiebe but does not expressly disclose the details of calculating the core position of the fingerprint.

Hara discloses ***preprocessing means which calculates coordinates and curvatures for a plurality of candidate points of the fingerprint information***

inputted by the biological information input device (column 2, lines 32-50 and column 6, lines 48-62 and column 7, lines 1-10).

Hara further discloses wherein a preprocessing means ***Calculates an average value of the coordinates for the plurality of candidate points*** (column 11, lines 53-66 and column 12, lines 5-19).

Hara further discloses wherein a preprocessing means ***determines a core position by the average value of the coordinates for the plurality of candidate points*** (column 12, lines 14-19).

Hara teaches a method of determining a core and Wiebe teaches that any fingerprint feature registration method deemed appropriate might be used in his registration (column 6, lines 5-9). Therefore it would have been obvious to one of ordinary skill in the art to use the core determination taught by Hara in combination with the fingerprint registration and access method taught by Wiebe to register fingerprints using the core determination.

Wiebe discloses the majority of the verification means including translational and rotational practices for correcting positional offsets in the fingerprints to be registered.

Hara teaches the calculation of a core position in a fingerprint using averages of coordinates. Although it should be obvious that the use of a core position determined by Hara in combination with the feature alignment taught by Wiebe would be useful in matching fingerprints, neither Hara nor Wiebe explicitly disclose using core position offset determination in matching fingerprints.

Iwata teaches calculating information for correcting positional offset and aligning two fingerprint images using a determined core position. The reference of Iwata is discussed here to teach that the use of a core position as determined by Hara would be used to determine the specifics of the offset correction disclosed by Wiebe.

Iwata discloses a method for biometric authentication similar to that of Wiebe by determining in the degree to which a captured fingerprint image (Fig. 1 and paragraph 0031, sentence 2 and page 11, line 18, the input fingerprint) matches a previously stored template (i.e. a registration fingerprint image). Like the Applicant's claimed invention, Iwata aligns the input fingerprint image and template using their respective core positions in order to facilitate subsequent matching procedures (page 8, paragraph 0026).

Iwata further discloses calculating information for correcting a positional displacement between said registered fingerprint and an input fingerprint that is newly input by using a core position of the fingerprints (page 9, lines 32-45, page 10, lines 1-5 and page 12, paragraph 0053). Specifically, Iwata extracts a singular point (e.g. the core – page 12, line 48) from each fingerprint (paragraph 0035). Then, using the extracted singular points aligns (i.e. correct for positional displacement of) the input fingerprint image with respect to the template, or vice versa (paragraph 0035). The alignment can be achieved by shifting one of the images so that the singular points of both images coincide (i.e. the positions of the extracted points are brought "into agreement" (page 10, paragraph 0035 and page 15, paragraph 0081). This process

effectively shifts each of the apertures (of the image undergoing correction) by an amount equal to the positional displacement between extracted singular points.

Once images have been aligned, they are compared to determine the degree to which they match (paragraph 0035).

Applicant has amended the independent claims to include the new limitations of:

wherein the transmitting means of the reader/writer comprises, for each partial image;

means for extracting from the input fingerprint a partial image requested by the requesting means of the mobile storage device, means for transmitting the extracted partial image to the mobile storage device, and means for repeatedly extracting and transmitting each of the partial images one by one until a satisfactory level of matching is achieved, and

wherein the judging means of the mobile storage device comprises:

means for repeating the matching result for each partial image.

As applicant states the difference between the newly claimed limitation and the primary reference to Wiebe is that Wiebe transfers the **entire pre-processed image** to the card for comparison with a template composed of several partial images while the present invention transfers **only partial images taken from a whole image** for performing the matching with the template.

Neither Wiebe Hara nor Iwata disclose transferring only partial images to be matched with a defined template.

Accordingly the new reference to U.S. Patent 6,241,288 to Bergenek et al. is cited to teach the claimed feature of determining correspondence of fingerprints using only partial images to match with a template. Bergenek discloses matching fingerprints in the same smart card environment (column 1, lines 15-25). Bergenek further discloses using partial images to determine if an inputted image matches a template image to a certain degree, wherein the template is made up of partial images as well (column 15, lines 42). Bergenek also teaches that the partial images are compared one by one in the discussion of outlying regions (column 15, lines 14-30).

Bergenek further teaches an advantage of using partial images instead of the entire fingerprint images if the security of not transmitting the entire fingerprint image. The added bonus of lessened computation time and expense in performing fewer pixel-to-pixel comparisons is also and obvious advantage. Therefore it would have been obvious to one of ordinary skill in the art at the time of invention to use the partial image matching taught by Bergenek in order to lessen computation time as well as provide added security.

Therefore it can now be seen that the references of Wiebe, Hara, Iwata and now Bergenek are combinable because it would have been obvious to one of ordinary skill in the art at the time of invention to use the core detection method of Hara in combination with the core matching and positional offset determination of Iwata in combination with the verification/access method of Wiebe in order to determine the correlation in the fingerprints used for verification/access process and it would have been obvious to use partial image/template registration as taught by Bergenek.

With regard to claim 5, Wiebe, Hara and Iwata disclose ***an authentication system according to claim 1.*** Wiebe further discloses ***wherein said reader/writer further comprises:***

Calculating means for calculating information for correcting a positional displacement between a registered fingerprint in said template and an input fingerprint that is newly input by forming images having specific luminance distribution in the peripheries of individual featuring points with regard to the input fingerprint, and by correlating said images there between (column 6, lines 15-27 and column 9, lines 1-13). As can best be determined from this claimed limitation, ***having specific luminance distribution in the peripheries of individual featuring points*** is interpreted as a "grey scale of sufficient quality" of the image (column 9, line 1). The correcting of positional offset is discussed in claim 1 (column 6, lines 15-27).

Wiebe further discloses ***retrieving means for retrieving a small image in the vicinity of a featuring point of said registered fingerprint is by matching in the vicinity of coordinates for an image of said inputted fingerprint, that wherein the positional displacement of the coordinates has been corrected*** (column 6, lines 16-27 and column 9, lines 15-26). Wiebe discloses comparing several small images within the fingerprint images used as a template and Wiebe also discloses positional displacement is performed.

Wiebe further discloses ***judging means for judging whether or not said fingerprint image is identical to said template according to the number of matched said small images*** (column 9, lines 50-67).

With regard to claim 6, Wiebe, Hara and Iwata disclose an authentication system according to claim 1, and Wiebe discloses ***wherein the calculation means for calculating an information for correcting a positional displacement*** (column 6, lines 17-28).

Hara discloses determining a ***core position by calculating other candidate points of the fingerprint information by calculating a coordinate of the candidate point of an initial position and a vector of ridge at the initial position of the candidate point*** (column 5, lines 20-35 and column 6, lines 40-62). Here Hara discloses finding tangential lines for the ridges and recording them. This is interpreted as vectors (Figs. 18 and 19). This kind of vector would be considered a tangential vector, which by definition would be orthogonal to a normal vector. These vectors or are used to determine curvature and finally core position.

Hara does not disclose the vectors to be normal vectors. It would be obvious to one of ordinary skill in the art that once tangential vectors are known it is only a logical step to calculate normal vectors should they be desired.

Iwata teaches that the local direction of a contour is defined in terms of its normal and tangent vectors within the aperture image (paragraphs 0056 and 0059). The singular point (e.g. the core of the fingerprint) is extracted based on the direction code

of each of the aforesaid aperture images (paragraph 0033 and 0067). Direction codes are predetermined (page 13, lines 39-41 and 0063). Core detection in Iwata is accomplished by retrieving a normal vector of a plurality of ridges sequentially, and determining a position where a direction of said normal varies from a predetermined value (pages 12-13, paragraphs 0052-0059, drawing 8). According to Iwata, the core located at a position in the fingerprint where ridge contours attain their maximum curvature (page 12, paragraph 0053). An abundance of prior art techniques exist for evaluating the curvature of contours, groups of contours, or vector fields, many of which utilize fields of normal vectors. Iwata for example, determines curvatures of ridge contours by evaluating their direction within each of the aperture images (paragraph 0055). Therefore it would have been obvious to one of ordinary skill in the art to use normal vectors as taught by Iwata, either in place of, or in combination with the tangential vectors taught by Hara to determine a core position of the fingerprints and to use the core position to calculate positional displacement as taught by Iwata for use in the access method of Wiebe.

With regard to claim 7, Wiebe, Hara and Iwata disclose an authentication system according to claim 1, and Hara discloses ***wherein the preprocessing means invalidates the candidate points having no more than a threshold value of curvature, and determines the core position by averaging the coordinates for the candidate points left over*** (column 12, lines 13-18). Hara discloses calculating a mean value to determine the core position. Here all points less than the threshold are

invalidated as all other candidate points less than the one maximum are invalidated. The left over point is therefore the core position.

With regard to claim 8, Wiebe, Hara and Iwata disclose an authentication system according to claim 1, and Wiebe discloses ***wherein the judging means judges identity of the fingerprint registered in the template and the input fingerprint, when a number of the match is no less than a threshold value*** (column 10, lines 1-4).

With regard to claim 9, Wiebe, Hara and Iwata disclose an authentication system according to claim 1, and Wiebe discloses ***wherein the private key is used for authentication of applications in a computer being connected to the reader/writer*** (column 5, lines 43-48). The operations that the processing unit is determined to be able to perform on the sensitive data is interpreted as authentication of applications in a computer connected to the reader/writer and the private key is again interpreted as the matching condition between reference biometric data and preprocessed biometric data. Wiebe further discloses checking the right to access sensitive material (column 3, lines 42-50 and column 1, lines 45-54). Once that right is checked, that act in itself can be interpreted as a key. The sensitive information stored on the smart card may include, though is clearly not limited to a "key" which makes it possible to open a door to access authorized data, so-called digital certificates (column 3, lines 42-50) or more

conventional information, such as a personal identification code or PIN (column 1, lines 50-54).

With regard to claim 10, Wiebe discloses ***a mobile storage device for authentication utilizing biometric information*** (column 3, lines 27-40 and Fig.1, element 1, smart card) ***the mobile storage device performing at least one of transferring read information to and receiving write information from a reader/writer*** (column 10, lines 10-15),

wherein the reader/writer comprises:

A biological information input device which inputs fingerprint information (Fig.1, element 8).

Wiebe further discloses ***wherein said mobile storage device comprises:***

A template which registers a plurality of coordinates of featuring points of the fingerprint and small images in vicinity of the coordinates (column 8, lines 51-59 and column 9, lines 44-65 and column 5, lines 12-20). Wiebe discloses using partial images as part of a template for registering the fingerprints. The coordinates are interpreted as being included in the registering known locations in the templates.

Wiebe further discloses ***a private key to be used for electronic authentication*** (column 3, lines 42-50 and column 1, lines 45-54). The sensitive information stored on the smart card may include, though is clearly not limited to a "key" which makes it possible to open a door to access authorized data, so-called digital certificates (column

3, lines 42-50) or more conventional information, such as a personal identification code or PIN (column 1, lines 50-54).

Wiebe further teaches the use of ***a transmitting means for transmitting the position generated in the preprocessing means to said mobile storage device according to a request from said mobile storage device*** (column 6, lines 39-47). The smart card has communication means capable of receiving and transmitting information. Using the determined position to align images is just one of many well-known methods used in the art to align and verify fingerprint images.

Wiebe further discloses a preprocessing means to calculate certain features of the fingerprint for comparison purposes (column 3, line 65-column 4, line 14 and column 5, lines 6-30).

Wiebe does not expressly disclose the preprocessing for determining curvatures coordinates and a core of the image from the average of the coordinates. Wiebe teaches that any method appropriate for the application for comparing feature information of fingerprint information may be used in the access method taught (column 6, lines 5-9).

Wiebe discloses ***preprocessing means for calculating coordinates or features of the fingerprint and rotating/translating the fingerprint to better register the stored fingerprint with the input fingerprint*** (column 5, lines 35-42 and column 6, lines 5-29), but does not disclose the details of calculating the coordinates and the core of the fingerprint. The calculation of coordinates is considered inherent to knowing the locations of feature points within the image with which to perform registration.

Hara teaches a method that uses ***preprocessing means which calculates coordinates and curvatures for a plurality of candidate points of the fingerprint information inputted by the biological information input device*** (column 2, lines 32-50 and column 6, lines 48-62 and column 7, lines 1-10).

Hara further teaches that the method ***calculates an average value of the coordinates for the plurality of candidate points, and determines a core position by the average value of the coordinates for the plurality of candidate points*** (column 11, lines 53-66 and column 12, lines 5-19);

Hara teaches a method of determining a core and Wiebe teaches that any fingerprint feature registration method deemed appropriate might be used in his registration (column 6, lines 5-9). Therefore it would have been obvious to one of ordinary skill in the art to use the core determination taught by Hara in combination with the fingerprint registration and access method taught by Wiebe to register fingerprints using the core determination.

Wiebe discloses the majority of the verification means including translational and rotational practices for correcting positional offsets in the fingerprints to be registered.

Hara teaches the calculation of a core position in a fingerprint using averages of coordinates. Although it should be obvious that the use of a core position determined by Hara in combination with the feature alignment taught by Wiebe would be useful in matching fingerprints, Neither Hara nor Wiebe explicitly disclose using core position

offset determination in matching fingerprints or, as claimed, ***calculating means for calculating an information for correcting a positional displacement based on a core position of a registered fingerprint recorded in said template and a core position of a registered fingerprint recorded in said template and a core position of an input fingerprint that is newly inputted, be referring to each said core position I the reader/writer.***

Iwata teaches calculating information for correcting positional offset and aligning two fingerprint images using a determined core position. The reference of Iwata is discussed here to teach that the use of a core position as determined by Hara would be used to determine the specifics of the offset correction disclosed by Wiebe.

Iwata discloses a method for biometric authentication similar to that of Wiebe by determining in the degree to which a captured fingerprint image (Fig. 1 and paragraph 0031, sentence 2 and page 11, line 18, the input fingerprint) matches a previously stored template (i.e. a registration fingerprint image). Like the Applicant's claimed invention, Iwata aligns the input fingerprint image and template using their respective core positions in order to facilitate subsequent matching procedures (page 8, paragraph 0026).

Iwata further discloses calculating information for correcting a positional displacement between said registered fingerprint and an input fingerprint that is newly input by using a core position of the fingerprints (page 9, lines 32-45, page 10, lines 1-5 and page 12, paragraph 0053). Specifically, Iwata extracts a singular point (e.g. the core – page 12, line 48) from each fingerprint (paragraph 0035). Then, using the

extracted singular points aligns (i.e. correct for positional displacement of) the input fingerprint image with respect to the template, or vice versa (paragraph 0035). The alignment can be achieved by shifting one of the images so that the singular points of both images coincide (i.e. the positions of the extracted points are brought "into agreement" (page 10, paragraph 0035 and page 15, paragraph 0081). This process effectively shifts each of the apertures (of the image undergoing correction) by an amount equal to the positional displacement between extracted singular points.

Once images have been aligned, they are compared to determine the degree to which they match (paragraph 0035).

Therefore it can now be seen that the references of Wiebe, Hara and Iwata are combinable because it would have been obvious to one of ordinary skill in the art at the time of invention to use the core detection method of Hara in combination with the core matching and positional offset determination of Iwata in combination with the verification/access method of Wiebe in order to determine the correlation in the fingerprints used for verification/access process.

Applicant has amended the independent claims to include the new limitations of:

wherein the transmitting means of the reader/writer comprises, for each partial image;

means for extracting from the input fingerprint a partial image requested by the requesting means of the mobile storage device, means for transmitting the extracted partial image to the mobile storage device, and means for repeatedly

extracting and transmitting each of the partial images one by one until a satisfactory level of matching is achieved, and

wherein the judging means of the mobile storage device comprises:

means for repeating the matching result for each partial image.

As applicant states the difference between the newly claimed limitation and the primary reference to Wiebe is that Wiebe transfers the **entire pre-processed image** to the card for comparison with a template composed of several partial images while the present invention transfers **only partial images taken from a whole image** for performing the matching with the template.

Neither Wiebe Hara nor Iwata disclose transferring only partial images to be matched with a defined template.

Accordingly the new reference to U.S. Patent 6,241,288 to Bergenek et al. is cited to teach the claimed feature of determining correspondence of fingerprints using only partial images to match with a template. Bergenek discloses matching fingerprints in the same smart card environment (column 1, lines 15-25). Bergenek further discloses using partial images to determine if an inputted image matches a template image to a certain degree, wherein the template is made up of partial images as well (column 15, lines 42). Bergenek also teaches that the partial images are compared one by one in the discussion of outlying regions (column 15, lines 14-30).

Bergenek further teaches an advantage of using partial images instead of the entire fingerprint images if the security of not transmitting the entire fingerprint image. The added bonus of lessened computation time and expense in performing fewer pixel-

to-pixel comparisons is also and obvious advantage. Therefore it would have been obvious to one of ordinary skill in the art at the time of invention to use the partial image matching taught by Bergenek in order to lessen computation time as well as provide added security.

Therefore it can now be seen that the references of Wiebe, Hara, Iwata and now Bergenek are combinable because it would have been obvious to one of ordinary skill in the art at the time of invention to use the core detection method of Hara in combination with the core matching and positional offset determination of Iwata in combination with the verification/access method of Wiebe in order to determine the correlation in the fingerprints used for verification/access process and it would have been obvious to use partial image/template registration as taught by Bergenek.

New Claims

With regard to claim 11, Wiebe discloses wherein a mobile storage device is an integrated circuit (IC) card (column 1, lines 28-42).

With regard to claim 12, the discussion of claim 1 applies. The only claimed limitation in claim 12 that is not also in claim 1 is the feature of ***a terminal connected with said reader/writer.*** Wiebe discloses a reader/writer (Fig. 1, element 2). Both the smart card and processing unit contain communication circuits for communicating.

These are circuits inherently contain terminals of some kind to enable the transfer of data.

8. Claims 13-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of U.S. Patent 6,719,200 to Wiebe, and U.S. Patent 6,241,288 to Bergenek et al.

With regard to claim 13, Wiebe discloses ***an authentication system comprising: a mobile storage device of a user; and a reader/writer for performing the reading of information from ands writing information into said mobile storage device*** (Fig. 1, element 2 and column 10, lines 10-15),

Wherein said reader/writer comprises:

An interface for transmitting and receiving information to and from said mobile storage device (Fig. 1, elements 3 and 4);

An input device for accepting the input of the biological information of said user (Fig. 1, element 8);

The following claimed elements are also listed:

A processing unit which performs a preprocessing on said biological information inputted through said input device, transmits a command for acquiring information to specify one partial image, extracts, one partial image corresponding to the information coming from said mobile storage device for

specifying said one partial image, from said mobile storage device, and receives the collation result of said one partial image, from said mobile storage device

Wherein said mobile storage device comprises:

An interface fro transmitting and receiving information to and from said reader/writer;

A storage device for storing a partial image of a biological information of said user registered in advance and the information for specifying said partial image; and

A processing unit which transmits, in response to said command from said reader/writer, the information fro specifying said one partial image in said storage device collates, in response to said one partial image from said reader/writer corresponding to the information for specifying said one partial image in said storage device, and transmits said collation result to said reader/writer, and

Wherein said processing unit of said reader/writer comprises:

Means for repeatedly transmitting said command, extracting said one partial image, transmitting said extracted one partial image, and receiving the collation result of said one partial image, for each partial image, until the matching number of partial images as a result of said collation exceeds a predetermined threshold value, and

Wherein said processing unit of said mobile storage device comprises:

Means for repeatedly transmitting the information for specifying said one partial image, collating said partial image, and transmitting said collation result, for each partial image.

An effort will now be made to summarize and explain the combination of references to Wiebe and Bergenek. It should also be noted that the two references are to the same assignee and would clearly be combinable as they solve the same fingerprint-matching problem in the same environment.

Wiebe discloses all the claimed elements of creating a template or predefined image on a smart card and then entering an image to be matched with the stored smart card template. See the discussion of the originally filed claims 1-10. Wiebe does not disclose the now claimed elements of matching the input fingerprint with the stored template by extracting only the partial images needed to do so. Wiebe's template is made up of only selected partial images, so in effect only partial images are matched, but Wiebe discloses sending the entire image to the smart card for matching rather than only extracting partial images one by one as claimed. Bergenek discloses a fingerprint-matching algorithm in the environment of smart cards and template matching (column 1, lines 15-25). Bergenek does not go into details about how the requests are made and where the data is when comparing the template on the card and the input image. Wiebe discloses all of these details as presently claimed. Bergenek further disclose performing the matching with a partial image template by extracting partial images from the input image one at a time and performing collation and also teaches that certain degrees of the collation can be determined, which includes matching for the purposes of

threshold collation determining (column 3, lines 18-38 and column 15, lines 13-30). Bergenek further discloses that the matching of the template and the partial images is performed on one reference region and then repeated for surrounding regions (column 3, lines 18-38).

Bergenek further teaches an advantage of using partial images instead of the entire fingerprint images if the security of not transmitting the entire fingerprint image. The added bonus of lessened computation time and expense in performing fewer pixel-to-pixel comparisons is also and obvious advantage. Therefore it would have been obvious to one of ordinary skill in the art at the time of invention to use the partial image matching taught by Bergenek in order to lessen computation time as well as provide added security.

Wiebe is cited to disclose the details of the smart card communication and Bergenek is cited to tech the use of partial image template matching. Therefore it can now be seen that the references of Wiebe, and Bergenek are combinable because it would have been obvious to one of ordinary skill in the art at the time of invention to use with the verification/access method and smart card embodiment of Wiebe in order to determine the correlation in the fingerprints used for verification/access process in combination with the use of partial image/template registration as taught by Bergenek.

With regard to claim 14, again Wiebe discloses the read/writer and mobile storage device or smart card as previously discussed.

Bergenek discloses wherein a processor ***detects, in said pre-processing, the position of one portion having a featuring constitution in said biological information, from said inputted biological information and sends out the one detected position*** (column 3, lines 18-30). Bergenek disclose finding a reference point, which is interpreted as a portion having a featuring constitution.

Bergenek further discloses ***wherein storage device further stores to position of one portion having the featuring constitution in said biological information*** (column 3, lines 20-30). Bergenek discloses creating a template and storing the reference point region in the template.

Bergenek further discloses ***wherein said processing unit of said mobile storage device calculates correction information for correcting the displacement between the position of one portion having a featuring constitution in said inputted biological information received from said writer/reader and the position of one portion having a featured constitution in the biological information stored in said device, corrects the information for specifying said partial image, with said correction information , and transmits the corrected information to said reader/writer*** (Figs. 12, 14 and 51 and column 13, lines 55-67 and column 14, lines 10-15 and 37-52). Bergenek discloses wherein a core position or position with featuring constitution is found and wherein that position information is used to find other feature regions. It is also disclosed that when a match is not acceptable for the center region, the image is rotated and/or positionally shifted in order to perform correlation.

With regard to claims 15 and 16, Bergenek also discloses detecting all featuring points and sends their positional or coordinate information for correlation (column 15, lines 14-30). Bergenek also discloses a point map for the featuring points in the form of a template (column 15, lines 15-25).

Bergenek further discloses comparing and correlating the featuring points and determining positional displacement giving the optimum correlation (column 15, lines 14-40 and column 14, lines 36-54).

With regard to claim 17, the discussion of claim 13 applies. Wiebe and Bergenek both disclose mobile storage devices for performing the fingerprint matching operation.

With regard to claim 18, the discussion of claim 18, the discussion of claim 14 applies.

With regard to claim 19, the discussion of claims 15 and 16 apply.

With regard to claim 20, Wiebe discloses an integrated circuit (IC) card (column 1, lines 28-35).

Referred

With regard to claim 21, the discussion of claim 13 applies.

Relevant Art

Another relevant reference to the Applicant's invention is the U.S. Patent Publication US 2004/0052405 to Walfridsson. The application discloses a very similar smart card, partial image template matching technique and is assigned to the same assignee as Bergenek and Wiebe. The reference does not however qualify as prior art because of the U.S. filing date.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Wes Tucker whose telephone number is 571-272-7427. The examiner can normally be reached on 9AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bhavesh Mehta can be reached on 571-272-2214. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Wes Tucker

4-11-06

MATTHEW C. BELLA
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600